Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire A
and Attestation of Compliance

Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced

Version 3.0

February 2014

Document Changes

Date	Version	Description
October 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0	To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0	To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.

Table of Contents

Before You Begin

SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;

- All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers;

- Your company has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;

- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;

- Your company has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**

- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Additionally, for e-commerce channels:

- The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

This SAQ is not applicable to face-to-face channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

PCI DSS Self-Assessment Completion Steps

1. Identify the applicable SAQ for your environment – refer to the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website for information.

2. Confirm that your environment is properly scoped and meets the eligibility criteria for the SAQ you are using (as defined in Part 2g of the Attestation of Compliance).

3. Assess your environment for compliance with applicable PCI DSS requirements.

4. Complete all sections of this document:

    - Section 1 (Part 1 & 2 of the AOC) – Assessment Information and Executive Summary.

    - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ A)

    - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)

5. Submit the SAQ and Attestation of Compliance, along with any other requested documentation— such as ASV scan reports—to your acquirer, payment brand or other requester.

Understanding the Self-Assessment Questionnaire

The questions contained in the "PCI DSS Question" column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS *(PCI Data Security Standard Requirements and Security Assessment Procedures)*	• Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	• Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	• Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*. Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.

Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that requirement. *Only one response should be selected for each question.*

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.

Response	When to use this response:
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. (See *Guidance for Non-Applicability of Certain, Specific Requirements* below for examples.) All responses in this column require a supporting explanation in Appendix C of the SAQ.

Guidance for Non-Applicability of Certain, Specific Requirements

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	Jubile Limited	DBA (doing business as):	N/A
Contact Name:	Petros Topouzis	Title:	CEO
ISA Name(s) (if applicable):		Title:	
Telephone:	+44 204 577 1290	E-mail:	petros.topouzis@jubile.tech
Business Address:	Kemp House, 160 City Road	City:	London
State/Province:	City of London	Country: United Kingdom	Zip: EC1V2NX
URL:	https://www.jubile.tech		

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	Zip:
URL:			

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☑ E-Commerce	☐ Mail order/telephone order (MOTO)

☐ Others (please specify):

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☑ E-Commerce	☑ E-Commerce
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

Note: If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	No CHD is stored, processed or transmitted by Jubile services or staff members.

Part 2c. Locations

List types of facilities and a summary of locations included in the PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.)

Type of facility	Location(s) of facility (city, country)
N/A	N/A

Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☐ Yes ☑ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	All credit card payments are processed by a third- party provider, Stripe, via a SAQ A- compliant iFrame embedded within the online customer store. No CHD is stored, processed or transmitted by Jubile services or staff members. All payment pages delivered to the customer's browser originate directly from Stripe.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☐ Yes ☑ No

Part 2f. Third-Party Service Providers

Does your company share cardholder data with any third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☑ Yes ☐ No

If Yes:

Name of service provider:	Description of services provided:
Stripe	Clearing and settlement of user payments

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

☑	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);
☑	All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers;
☑	Merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
☑	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☑	Merchant has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☑	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.
☑	*Additionally, for e-commerce channels:* The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

Section 2: Self-Assessment Questionnaire A

Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures *document.*

Self-assessment completion date:

Requirement 9:   Restrict physical access to cardholder data

	PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
			Yes	**Yes with CCW**	**No**	**N/A**
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	▪ Review policies and procedures for physically securing media ▪ Interview personnel	☐	☐	☐	☒
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	▪ Review policies and procedures for distribution of media	☐	☐	☐	☒
	(b) Do controls include the following:					
9.6.1	Is media classified so the sensitivity of the data can be determined?	▪ Review policies and procedures for media classification ▪ Interview security personnel	☐	☐	☐	☒
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	▪ Interview personnel ▪ Examine media distribution tracking logs and documentation	☐	☐	☐	☒
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	▪ Interview personnel ▪ Examine media distribution tracking logs and documentation	☐	☐	☐	☒
9.7	Is strict control maintained over the storage and accessibility of media?	▪ Review policies and procedures	☐	☐	☐	☒

PCI DSS SAQ A, v3.0 − Section 2: Self-Assessment Questionnaire
© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

February 2014
Page 4

Document Ref: JXVTJ-ZPRO2-A6POY-PC7KN

Page 10 of 19

	PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	▪ Review periodic media destruction policies and procedures	☐	☐	☐	▣
	(c) Is media destruction performed as follows:					
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	▪ Review periodic media destruction policies and procedures ▪ Interview personnel ▪ Observe processes	☐	☐	☐	▣
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	▪ Examine security of storage containers	☐	☐	☐	▣

Maintain an Information Security Policy

Requirement 12:   Maintain a policy that addresses information security for all personnel

Note: *For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	**Yes with CCW**	**No**	**N/A**
12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:					
12.8.1 Is a list of service providers maintained?	▪ Review policies and procedures ▪ Observe processes ▪ Review list of service providers	☒	☐	☐	☐
12.8.2 Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? **Note:** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	▪ Observe written agreements ▪ Review policies and procedures	☒	☐	☐	☐
12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☒	☐	☐	☐
12.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☒	☐	☐	☐

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☑	☐	☐	☐

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	**Explanation**
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
3.4	Cardholder data is never stored electronically
9.5, 9.6, 9.6.1 - 9.6.3, 9.7, 9.8, 9.81	Jubile does not process cardholder data electronically or in paper form. The use of media, for cardholder data is not applicable.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated *(completion date)*, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of *(date)*: (**check one**):

☑	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

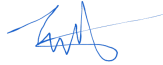|	
☑	PCI DSS Self-Assessment Questionnaire A, Version *(version of SAQ)*, was completed according to the instructions therein.
☑	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☑	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☑	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☑	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

☑	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *(ASV Name)*

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer ↑	*Date:*	2021-11-10
Merchant Executive Officer Name: Petros Topouzis	*Title:*	CEO

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of QSA ↑	*Date:*
QSA Name:	*QSA Company:*

Part 3d. ISA Acknowledgement (if applicable)

If a ISA was involved or assisted with this assessment, describe the role performed:	

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

---

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	**NO**	
9	Restrict physical access to cardholder data	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	

Signature Certificate

Document Ref.: JXVTJ-ZPRO2-A6POY-PC7KN

Document signed by:

Petros Topouzis

E-mail:
petros.topouzis@jubile.tech

Signed via link

IP: 93.105.178.194 Date: 10 Nov 2021 20:12:31 UTC

Document completed by all parties on:
10 Nov 2021 20:12:31 UTC

Page 1 of 1